Framing a human rights approach to communication surveillance laws through the African human rights system in Nigeria, South Africa and Uganda

*Tomiwa Ilori**
https://orcid.org/0000-0002-2765-3103

ABSTRACT: Today, in any society where crime is possible, communication surveillance is a necessary evil. This is because technologies now offer faster means of preventing crime while they are also capable of undermining the right to privacy. However, protecting privacy should not be mutually exclusive of ensuring public safety. This article argues that while communication surveillance may be permissible under narrow and limited circumstances, the laws made to regulate it in Nigeria, South Africa and Uganda do not comply with international human rights standards. In demonstrating this, this article analyses the major laws in these countries alongside the various international human rights principles that must be complied with in framing a rights-respecting law on communication surveillance. The major contribution of this article is that communication surveillance laws can be designed in compliance with international human rights standards in the countries under focus. These include Nigeria, South Africa and Uganda carrying out specific legal reforms targeted at problematic laws on communication surveillance in order to bring them in line with international human rights standards. This can also be supported by developing a more robust set of comprehensive guidelines through the African Commission and Human and Peoples' Rights and ensuring that Nigeria, South Africa and Uganda embark on critical and strategic training for stakeholders involved in the enforcement and implementation of communication surveillance laws in these countries.

TITRE ET RÉSUMÉ EN FRANCAIS:

Définir une approche des droits de l'homme à la législation sur la surveillance des communications à travers le système africain des droits de l'homme au Nigeria, en Afrique du Sud et en Ouganda

RÉSUMÉ: Aujourd'hui, dans toute société où la criminalité est possible, la surveillance des communications est un mal nécessaire. Alors que les technologies offrent désormais des moyens de prévention des crimes plus rapides, elles demeurent tout autant capables de porter atteinte au droit à la vie privée. Cependant, la protection de la vie privée ne devrait pas être incompatible avec la sécurité publique. Cet article soutient que si la surveillance des communications peut être autorisée dans des circonstances étroites et limitées, les lois adoptées pour la réglementer au Nigeria, en Afrique du Sud et en Ouganda ne sont pas conformes aux normes internationales en matière de droits de l'homme. Pour le démontrer, cet article analyse les principales lois de ces pays ainsi que les différents principes internationaux des droits de l'homme qui doivent être respectés dans l'élaboration d'une loi sur la surveillance des communications respectueuse des droits. La principale contribution de cet article est que les lois sur la surveillance des communications peuvent être conçues en

* LLB (Hons); LLM (Pretoria); Doctoral candidate, Centre for Human Rights, Faculty of Law, University of Pretoria; tomiwailori@gmail.com

T Ilori 'Framing a human rights approach to communication surveillance laws through the African human rights system in Nigeria, South Africa and Uganda'
(2021) 5 *African Human Rights Yearbook* 134-157
http://doi.org/10.29053/2523-1367/2021/v5a7

conformité avec les normes internationales des droits de l'homme dans les pays sous examen. Il s'agit notamment pour le Nigeria, l'Afrique du Sud et l'Ouganda de mener des réformes juridiques spécifiques visant les lois problématiques sur la surveillance des communications afin de les rendre conformes aux normes internationales en matière de droits de l'homme. Cela peut également être soutenu par le développement d'un ensemble plus robuste de lignes directrices complètes par la Commission africaine des droits de l'homme et des peuples et en s'assurant que le Nigeria, l'Afrique du Sud et l'Ouganda s'engagent dans une formation critique et stratégique des parties prenantes impliquées dans l'application et la mise en œuvre des lois sur la surveillance des communications dans ces pays.

KEY WORDS: communication surveillance, lawful interception, privacy, human rights approach, legal reforms, Nigeria, South Africa, Uganda

CONTENT:

1 INTRODUCTION

At no time has the phrase 'information is power' become more resounding than the turn of the last century. Access to technologies has since increased in many parts of Africa while also bringing with them renewed hopes of political, social and economic liberation.[1] However, as the promises of these technologies becomes bolder, especially in Africa, their threats to human rights have also increased due to human rights violations by state and non-state actors.[2] In addition to these threats, global needs, both in technological developments and maintaining peace and security, have also challenged the meaning of human rights protection especially in the digital age.[3] While in the past,

1 M Manacorda & A Tesei 'Liberation technology: mobile phones and political mobilization in Africa' (2020) 80 *Econometrica* 564; C Dendere 'Tweeting to democracy: a new anti-authoritarian liberation struggle in Zimbabwe' (2019) 38 *Cadernos de Estudos Africanos* 179-187; D Mwambari 'Can online platforms be *e-Pana-Africana Liberation Zones* for pan-African and decolonization debates?' (2021) 5 *CODESRIA Online Bulletin*.

2 H Dube, MA Simiyu & T Ilori 'Civil society in the digital age in Africa identifying threats and mounting pushbacks' (2020) Centre for Human Rights, University of Pretoria https://media.africaportal.org/documents/Civil_society_in_the_digital_age_in_Africa_2020.pdf (accessed 23 April 2021).

3 E Marmo 'Human rights in the digital age: challenging issues in the UN agenda' *Global Policy Forum* 6 April 2020 https://www.globalpolicywatch.org/wp-content/uploads/2020/04/20200406-UN-Monitor-14-Human-Rights-Digital-Technologies.pdf (accessed 5 May 2021).

states have been known more for their roles in deploying communication surveillance,[4] today, they are joined by an entire economy of innovative ideas, emboldened by non-state actors that thrive on predicting human interaction as a source of revenue.[5] The kind of communication surveillance we know originally as state-designed 'backends' now include blatant manipulation of human online behaviour and snooping on private communication by online platforms. As a result, digital technologies have not only brought new challenges, the idea of socio-political power which drives today's democratic developments is now concentrated in fewer private behemoths.[6] Most actors justify communication surveillance on the basis of the need to ensure public safety, prevention of crime, protecting the rights of others, and ensuring national security, while they downplay the negative impacts these justifications have on human rights like privacy.[7]

In most African countries, despite state parties' obligations under international human rights system especially on the use of communication surveillance, there is no comprehensive set of rules on the subject both at the regional and domestic level. While a number of global and regional human rights instruments provide direction on the major principles state parties must consider in the deployment of communication surveillance, currently, most state parties do not have a comprehensive, primary and human rights-compliant laws on communication surveillance.[8] For the state parties who have such laws, while they may appear comprehensive and made by the national parliaments, they are not compliant with respect to internationally set principles on communication surveillance.[9]

In framing a human rights basis for communication surveillance within the African context, this article considers the major principles under the African human rights system. It analyses how these principles are complied with by three state parties: Nigeria, South Africa and Uganda. It then considers the gaps in the major laws that regulate communication surveillance in these countries and gives

4 T Weller 'The information state: a historical perspective on surveillance' in K Ball, KD Haggerty, & D Lyon (eds) *Routledge handbook on surveillance studies* (2012) 57-63.

5 S Zuboff 'Surveillance capitalism and the challenge of collective action' (2019) 28 *New Labor Forum* 10-29.

6 As above.

7 J Wirth, C Maier & S Laumer 'Justification of mass surveillance: a quantitative study' (2019) *14th International Conference on Wirtschaftsinformatik, February 24-27, 2019, Siegen, Germany* 1346-1348; JB Rule '"Needs" for surveillance and the movement to protect privacy' in K Ball, KD Haggerty & D Lyon (eds) *Routledge handbook on surveillance studies* (2012) 54-71.

8 Collaboration on international ICT policy in East and Southern Africa (CIPESA) 'Mapping and analysis of privacy laws and policies in Africa: summary report' (2021) https://cipesa.org/?wpfb_dl=454 (accessed 5 September 2021).

9 Under the analysis under section 6, South Africa's surveillance law seems to fare better compared to other laws in Nigeria and Uganda given the recent 'cure' by the South African Constitutional Court's recent judgment in the *Amabhungane* case. However, despite this judgment, the law does not provide for other aspects needed for human rights protection. See section 6 below.

recommendations on how these countries can bring their communication surveillance laws in line with international human rights standards. It is important to note that this article is neither a conclusive position on communication surveillance and human rights in Africa nor a presentation of exhaustive solutions to the challenges being faced in ensuring human rights-complaint laws with respect to communication surveillance. Rather, it is an exercise in fortitude and strategy for necessary reforms in the area of communication surveillance in Africa — to have major stakeholders rethink the growing need to protect the right to privacy, specifically, and human rights, in general, in the face of intrusive and invasive digital technologies.

In considering these issues, this article analyses academic literature, international human rights treaties and mechanisms and various laws especially on how they intersect with the deployment of communication surveillance. Particularly, it draws on the recently revised Declaration of Principles on Freedom of Expression and Access to Information in Africa (revised Declaration) on how state parties should design policies on communication surveillance.[10] It also considers various reports and studies by international organisations, newspapers and other reliable sources.

In terms of structure, this article is divided into seven sections. The first section provides a background for the article while the second section provides a brief overview of communication surveillance especially within the African context and what it means when considered alongside other terms like surveillance, lawful and unlawful interception of communication. The third section examines current international human rights law on communication surveillance after which it focuses its analyses on the African context. The fourth section highlights the relationship between the revised Declaration and an elaborate set of 13 principles for framing a human rights approach to communication surveillance.

The fifth section analyses communication surveillance, especially through various lawful interception laws in Nigeria, South African and Uganda to draw out the need for a more comprehensive, primary and human rights-compliant policies on communication surveillance practices. The sixth section makes recommendations on ways forward and how state parties can frame and ensure their compliance with internationally-set standards on communication surveillance in the region. The final section concludes that while laws that regulate communications surveillance in Nigeria, South Africa and Uganda may be non-compliant with internationally set standards, there are ways to bring them into line with these standards to achieve the twin-objective of using communication surveillance and protecting the right to privacy.

10 African Commission 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2019) https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf (accessed 23 July 2021).

2 PLACING COMMUNICATION SURVEILLANCE IN CONTEXT

Communication surveillance is broader in scope than lawful interception of communication just as surveillance is broader in scope than communication surveillance.[11] However, these aspects of surveillance all form an arc that bends towards the right to privacy. In general, communication surveillance includes lawful or unlawful access to electronic communication.[12] Lawful access to electronic communication largely refers to the legal and legitimate basis for monitoring and gaining access to private communications. In other words, it would qualify as lawful interception of communication if gaining access to such private communication has a high possibility of forestalling an irreparable harm to life and property. Some of the reasons for communication surveillance include the need to ensure public safety, prevention of crime, protecting the rights of others and even mutual assistance between countries with respect to fighting crime.

Due to the nature of communication surveillance, especially in its use by governments, it often requires a level of secrecy. As noted by Smith:[13]

> Most varieties of surveillance operation are governed by stringent secrecy directives, companies seemingly as keen to extract and capture informational flows as they are to prevent and prohibit everyday work practices from being directly inspected and made transparent.

Such secrecy includes instances where the government must carry out investigation with respect to reasonable suspicion of crime and notifying either the subject(s) of investigation or the general public of such surveillance might jeopardise the investigation. However, this need seems to have obscured the need for accountability and transparency which as a result leads to violations of privacy rights specifically and human rights in general.[14]

A report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression defines 'communications surveillance' as 'the monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communications network'.[15] The report also noted that issues such as national security and criminal

11 Media Policy and Democracy Project 'The surveillance state: communications surveillance and privacy in South Africa' (2016) https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf (accessed 23 July 2021); LA Abdulrauf 'The challenges for the rule of law posed by the increasing use of electronic surveillance in sub-Saharan Africa' (2018) 18 *African Human Rights Law Journal* 368.

12 HW Gebreegziabher 'The right to privacy in the age of surveillance to counter terrorism in Ethiopia' (2018) 18 *African Human Rights Law Journal* 401.

13 GJ Smith 'Surveillance work(ers)' in K Ball, KD Haggerty & D Lyon (eds) *Routledge handbook on surveillance studies* (2012) 109.

14 AD Moore 'Privacy, security, and government surveillance: wikileaks and the new accountability' (2011) 25 *Public Affairs Quarterly* 15.

activity may justify the exceptional use of communications surveillance technologies and what this suggests is that lawful interception of communication as a major component of communication surveillance could be an accepted basis for limiting the right to privacy.[16] Due to the nature of communication surveillance, states are enjoined to ensure that such limitation is based on the principles of international human rights law.

3 INTERNATIONAL HUMAN RIGHTS LAW AND COMMUNICATION SURVEILLANCE IN AFRICA

The international human rights system as organised at the level of the United Nations (UN) and various other regional human rights systems have provided guidance on how states who have the primary responsibilities of protecting human rights can develop rights-respecting policies on communication surveillance.[17] On the relationship between the right to privacy under the International Covenant on Civil and Political Rights (ICCPR) and communication surveillance, Diggelmann and Cleis argue that the primary aspects of the right focus on freedom from society and privacy as dignity,

> the drafting history of the right to privacy does not allow for the conclusion that one of the two competing ideas can claim the status of the primary idea. Rather, it seems to support the view that the very concept of privacy is inextricably linked to more than one idea.[18]

In understanding communication surveillance as being inextricably linked to the right to privacy, in its the General Comments 16 on article 17 of the ICCPR by the Human Rights Committee, 'surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.'[19] In the commentary that provides an in-depth analysis of the ICCPR, privacy, under international human rights law 'covers all forms of communication over distance, i.e., by telephone, telegram, telex, e-mail, and other mechanical or electronic means of communication.'[20]

15 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations Human Rights Council (17 April 2013), UN Doc A/HRC/23/40 (2013).

16 Report of the Special Rapporteur on the right to privacy, United Nations Human Rights Council (6 September 2017) UN Doc A/HRC/23/40 (2017); United Nations Human Rights Council (n 15) 3.

17 Privacy International 'Guide to international law and surveillance 2.0' (2019) https://privacyinternational.org/sites/default/files/2019-04/Guide%20to%20International%20Law%20and%20Surveillance%202.0.pdf 3-5 (accessed 23 July 2021).

18 O Diggelmann & MN Cleis 'How the right to privacy became a human right' (2014) 14 *Human Rights Law Review* 458.

19 The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, UN Human Rights Committee, CCPR General Comment 16: Article 17 (Right to Privacy).

With respect to the ICCPR, article 17 provides for the right to privacy as follows:

> (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> (2) Everyone has the right to the protection of the law against such interference or attacks.

In addition to this, article 4(2) of the ICCPR makes provisions for rights that may be derogated from in case of public emergency which may also include the right to privacy. It has also been noted that in limiting the right to privacy, the limitative tests like legality, legitimacy, proportionality and necessity provided for other rights like the right to liberty of movement and freedom to choose residence; freedom of thought, conscience and religion; peaceful assembly; and freedom of association would apply.[21] The four jointly applicable requirements for limitation of privacy rights with respect to communication surveillance are that such need must not be:

> (a) arbitrary and must be provided for by law;
>
> (b) for any purpose but for one which is necessary in a democratic society;
>
> (c) for any purpose except for those of 'national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others'; and,
>
> (d) [dis]proportionate to the threat or risk being managed.

This means that for a legislative framework on communication surveillance to be rights-respecting, it must be provided for by law, be necessary, legitimate and proportionate to the harm sought to be managed.

The African Charter on Human and Peoples' Rights does not provide explicitly for the right to privacy as a substantive right.[22] However, its framing of the right and its necessity given the challenges posed by the digital age and communication has demonstrated the need to read the right and its various aspects into both the promotional and protective mandates of the implementing institutions within the African human rights system. For example, the right is provided for by various thematic human rights instruments like article 10 of the African Charter on Rights and Welfare of the Child,[23] article 7 of the African Youth Charter[24] and Chapter 2 of the African Union Convention on Cybersecurity and Personal Data.[25]

In addition to these, the African Commission on Human and Peoples' Rights revised the Declaration of Principles of Freedom of

20 M Nowak *UN Covenant on Civil and Political Rights: CCPR commentary* (2005) 401.

21 United Nations Human Rights Council (n 15) para 28.

22 African Charter on Human and Peoples' Rights (1981) https://www.achpr.org/legalinstruments/detail?id=49 (accessed 24 June 2021).

23 African Charter on Rights and Welfare of the Child (1990) https://www.achpr.org/public/Document/file/English/achpr_instr_charterchild_eng.pdf (accessed 22 June 2021).

24 African Youth Charter (2006) https://au.int/sites/default/files/treaties/7789-treaty-0033_-_african_youth_charter_e.pdf (accessed 22 June 2021).

Expression and Access to Information in Africa (revised Declaration).[26] The revised Declaration is a 'soft law' instrument which is developed to guide states on major topical issues including developing laws and policies with respect to the right to freedom of expression, access to information and the right to privacy in Africa.[27] Additionally, the body of international human rights instruments expatiated on in the report by Privacy International above[28] can be received into the African human rights system by virtue of provisions of article 60 of the African Charter that allows the African Commission to read international human rights instruments into its jurisprudence and activities.

While a number of human rights like freedom of expression, association and assembly are interconnected with the use of communication surveillance, the right to privacy seem the most proximate. This is because 'being watched' whether in real-time or indirectly through retained data impact on the right of an individual or a group of people to be without unwarranted interference. In this regard, Principles 40-42 of the Revised Declaration has provisions on how states must protect not only the right to privacy but also its other aspects in the digital age like communication surveillance and protection of personal information. Principle 41 of the revised Declaration provides for the responsibilities of states with respect to communication surveillance and protection of privacy rights:

(1) States shall not require internet intermediaries to proactively monitor content which they have not authored or otherwise modified.

(2) Everyone has the right to privacy, including the confidentiality of their communication and the protection of their personal information.

(3) Everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communication and personal information from access by third parties through the aid of digital technologies.

(4) States shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communication.

(5) States shall only engage in targeted communication surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.

(6) States shall ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy, including:

  (a) the prior authorisation of an independent and impartial judicial authority;
  (b) due process safeguards;
  (c) specific limitation on the time, manner, place and scope of the surveillance;
  (d) notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;
  (e) proactive transparency on the nature and scope of its use; and

25 African Union Convention on Cybersecurity and Personal Data (2014) https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 22 June 2021).

26 African Commission (n 10).

27 African Commission (n 10) Preamble.

28 Privacy International (n 17).

(f) effective monitoring and regular review by an independent oversight mechanism.

In the analyses carried out by the Electronic Frontier Foundation (EFF) and article 19, both civil society organisations focused on the impacts of communication surveillance on human rights.[29] It was noted that 'all information relating to a person's private communication should be considered to be 'protected information,' and should accordingly be given the strongest legal protection. The analyses, which were based on international human rights law with respect to communication surveillance, identified at least 13 major principles that must be considered in designing human rights policies on communication surveillance.

These 13 principles for a human rights approach to communication surveillance are directly sourced from the four jointly applicable requirements for limitation of rights under the ICCPR. These four basic principles are further elaborated through 13 principles which are legality; legitimate aim; necessity; adequacy; proportionality; competent judicial authority; due process; 'user notification'; the right to an effective remedy; transparency; public oversight; integrity of communication and systems; safeguards for international cooperation; and safeguards against illegitimate access. These principles justify their relevance through 'case law and views of a range of international human rights bodies and experts, such as UN special rapporteur.'[30] Due to the interrelationship and interdependence of these principles, they are applicable jointly and compliance with one does not mean compliance with the entire standards as established under international human rights law.

While only Morocco has not ratified the African Charter,[31] Nigeria, South Africa and Uganda have various obligations under treaties to ensure the implementation of the rights contained in instruments especially with respect to communication surveillance and privacy. In many instances, communication surveillance is regulated through laws on lawful interception. In framing communication surveillance with a human rights approach, not only must policies be compliant with specific obligations like the four-part test, they should ensure transparency and accountability.

29 Electronic Frontier Foundation (EFF) & art 19 'Necessary & proportionate international principle on the application of human rights to communications surveillance: Background and supporting international legal analysis' May 2014 https://www.article19.org/data/files/medialibrary/37564/N&P-analysis-2-final.pdf (accessed 25 May 2021).

30 EFF & art 19 (n 29) 10.

31 United Nations Human Rights, Office of the High Commissioner 'Status of ratification' https://indicators.ohchr.org/accessed 25 May 2021; Ratification Table: African Charter on Human and Peoples' Rights https://www.achpr.org/ratificationtable?id=49 (accessed 25 May 2021).

4 THE REVISED DECLARATION AND FRAMING A HUMAN RIGHTS APPROACH FOR A COMMUNICATION SURVEILLANCE FRAMEWORK

The goal of this section of the article is to make a firmer connection between the four-part test for permissible restriction of the right to privacy, Principle 41 of the revised Declaration on states' responsibility with respect to communication surveillance and a set of 13 carefully developed elaborate principles for ensuring rights-respecting laws for communication surveillance. This connection foregrounds how a human rights approach to laws on communication surveillance within the African context can be framed. The significance of the strong relationship between the four-part test, the revised Declaration and the 13 principles is seen in how it could assist states in finding the conceptual and contextual relevance of international human rights law to communication surveillance in African countries.

This is because states have often criticised the broadness of international human rights principles especially when compared to its specific application on the ground in their respective systems.[32] For example, in what ways can communication surveillance be employed in the midst of pressures of insecurity? Here, a more robust set of legal principles on communication surveillance would assist states to understand when their legislative policies on lawful interception does not comply with international human rights law. This will not only assist with conceptual clarity on what such compliance means, it would also assist with contextual application in order to assess the compliance of the law with international human rights standards.

On a closer look, Principle 41 has striking similarities with both the four jointly applicable requirements for limitation of rights under the ICCPR and the 13 major principles for designing a legal framework on communication surveillance. Starting with the legality principle, in order to fulfil the requirement of it being clear and sufficiently precise, it has seven sub-principles that a framework on communication surveillance must comply with. These sub-principles also find expression in the provisions of Principle 41 of the revised Declaration. In order for a law on communication surveillance to comply with the principle of legality, it must define the offences and activities where surveillance may be carried out; provide for the categories of people that may subject to surveillance; prescribe a time-limit on surveillance operations; ensure due process; ensure examination, use and storage of surveillance data; provide for precautions with respect to sharing surveillance data with third party; provide for destruction or erasure of surveillance data; and provide for independent supervisory authority appointed by and responsible to the legislature.[33]

32 F Viljoen 'Contemporary challenges to international human rights law and the role of human rights education' (2011) 44 *De Jure* 209.

There are at least five examples of where it could be permissible to limit the right to privacy based on the principle of legitimacy with respect to communication surveillance. They are public safety; prevention of crime; ensuring public morals; protecting the rights of others; ensuring national security and economic well-being of individuals. This could be the basis provided for under Principle 41(5) of the revised Declaration which could also be referred to as the basis for the requirements of necessity, adequacy and proportionality.

In determining proportionality and necessity, there are also the requirements for judicial overview and due process which are further subdivided into prior authorisation; retroactive authorisation; and internal judicial checks for *ex-parte* orders which may all be connected to the provisions of Principle 41(6)(a) of the revised Declaration. Prior authorisation may be regarded as the general rule for communication surveillance where the approval of a designated judge is obtained before surveillance is carried out. There are instances where it is clearly impossible to obtain an approval of a designated judge before carrying out interception of communication due to imminent threats to lives and properties. In such instances, a law enforcement agency may carry out such surveillance but must immediately inform such designated judge within a particular period for approval or otherwise for such interception. In addition to this, due to the nature of communication surveillance especially in relation to the surveilled subjects and obtaining a designated judge's approval, there are chances that such request for surveillance would be heard *ex parte* – in the absence of the surveilled subject. Therefore, it is necessary that a legal practitioner should be appointed to argue for the interests of the surveilled subject, hence the need for internal judicial checks for granting such surveillance requests.

Additionally, 'user notification', that is, the need for a surveilled subject to be informed of when they have been surveilled and the right to effective remedy are principles that a law for lawful interception must provide for. 'User notification' ensures that in instances where the privacy rights of a surveilled subject has been violated, they are in a position to make a decision as to whether they would seek effective remedy for such violation or not. There is also the requirement for transparency where states must ensure that the laws are clear especially in how it is implemented and providing accessible means for monitoring such implementation. Such laws should also allow for public oversight where not only the information on surveillance is shared by states with the public but also should be mandated by service providers. Both requirements for 'user notification' and transparency may also be found in the provisions of Principle 41(6)(d) and (f) of the revised Declaration respectively.

A law on communication surveillance should also provide for the integrity of communications and systems which is in line with Principle

33 Principle 41(5); Principle 41(4) & Principle 41(6)(c); Principle 41(6)(c); Principle 41(4); Principle 41(3); Principle 41(4); and Principle 41(6)(f) of the revised Declaration.

41(3) of the revised Declaration. In addition, there should be adequate guidelines in instances where states must engage in international cooperation that is not only mutual in terms of interests but mutual because of the need to protect human rights in line with Principle 41(5) of the revised Declaration. Finally, laws should provide safeguards against illegitimate access of communications at least in three major ways. First, by not requiring that service providers to facilitate interceptable communications in line with Principle 41(1) of the revised Declaration, second by not requiring the decryption of communications in line with Principle 41(2) of the revised Declaration and third by ensuring that illegally obtained interception is not admissible in a court proceeding as provided for under Principle 41(4) of the revised Declaration. These principles, fleshed out and elaborate, demonstrate internationally-set basic principles laws on communication surveillance must provide for. However, as it would be shown in the subsequent sections, some of these principles are not provided for in Nigeria, South Africa and Uganda.

5 AN ASSESSMENT OF COMMUNICATION SURVEILLANCE LAWS IN NIGERIA, SOUTH AFRICA AND UGANDA

5.1 An overview of communication surveillance landscape in Nigeria

In Nigeria, aside from the provisions of section 37 of the 1999 Constitution on the right to privacy, there are a number of other laws that impact on the right to privacy especially through their provisions on communication surveillance. The major laws are the Cybercrimes (Prohibition, Prevention) Act, 2015, the Nigerian Communications (Enforcement Process, etc) Regulations, 2019, Guidelines on Provision of Internet Services, the NCC Act, section 26(1) of the Terrorism (Prevention) Act, 2011 (as amended) and section 13 of the Mutual Assistance in Criminal Matters Within the Commonwealth (Enactment and Enforcement) Act, 2019.[34] The Lawful Interception of Communications Regulations, 2019 (Regulations) is the most comprehensive law with respect to communication surveillance law in Nigeria.[35] Most of these laws provide for lawful interception especially as it relates to their various objectives. For example, the Terrorism Act

34 Sec 38, The Cybercrimes (Prohibition, Prevention) Act, 2015; Regulation 8(2)(a) Nigerian Communications (Enforcement Process, etc) Regulations, 2019; Guideline 6(c) Guidelines of Provision of Internet Services; Section 148(1)(c) Insert NCC Act; Section 26(1) Terrorism (Prevention) Act, 2011 (accessed 18 March 2020), Section 13 Mutual Assistance in Criminal Matters Within the Commonwealth (Enactment and Enforcement) Act, 2019, (accessed 22 June 2020).

35 Lawful Interception of Communications Regulations, 2019 (Regulations) https://www.ncc.gov.ng/accessible/documents/839-lawful-interception-of-comunications-regulations-1/file (accessed 22 June 2020).

provides for interception of communications with respect to investigating terrorist activities. It is important to note that while most of these laws provide for the powers of law enforcement to intercept communications, they rarely provide for accountability, transparency or any specific steps towards human rights protection in the exercise of such powers.[36]

This is particularly problematic in that in a report which considers the investment of the Nigerian government on surveillance equipment between 2014-2017, the government has spent ₦127,000,000,000.00 (approximately US$308 582 187,00) without any clear guidance as to the deployment of these equipment.[37] In addition to these investments, there have also been recent reports that Nigeria is one of the seven African countries heavily invested in the use of spyware and intrusive technologies.[38] This report corroborates other reports on how the Nigerian government surveils journalists and political opponents.[39] These can be attributed to lack of transparency and accountability on lawful interception in Nigeria.

5.1.1 The Lawful Interception of Communications Regulations, 2019 (Regulations)

The provisions of the Regulations are made pursuant to the provisions of sections 70, 146 and 147 of the Nigerian Communications Act, 2003 with respect to the powers of the Nigerian Communications Commission (NCC) to publish regulations on provisions of the Act, general duties of licensees and interception of communications respectively. This makes the Regulations a secondary law on surveillance in Nigeria. The objectives of the Regulations 'included to ensure that the privacy of subscribers' communication as provided for in the Constitution of Nigeria is preserved'.[40]

The Regulations are divided into six sections: scope, objectives, regulations; interception of communications; protected or encrypted communications; interception capabilities; administration of lawful interceptions of communications; and miscellaneous. Considering the Regulations' compliance with respect to international human rights standards, there are a number of issues on how they may pose threats to the right to privacy through communication surveillance.

36 Out of these laws, only the Regulations provide for some oversight responsibilities in the Attorney-General of the Federation. None of the laws make any adequate provisions with respect to human rights protection. See section 5.1.2 on more analysis on the Regulation.

37 T Ilori 'Status of surveillance in Nigeria: refocusing the search beams' (2017) https://paradigmhq.org/wp-content/uploads/2021/04/Policy-Brief-009-Status-of-Surveillance-in-Nigeria.pdf (22 June 2020).

38 B Marczak & others 'Running in circles: uncovering the clients of cyberespionage firm Circles' 1 December 2021, https://tspace.library.utoronto.ca/bitstream/1807/106212/1/Report%23133--runningincircles.pdf (accessed 23 June 2021).

39 J Rozen 'How Nigeria's police used telecom surveillance to lure and arrest journalists' 13 February 2020, https://cpj.org/2020/02/nigeria-police-telecom-surveillance-lure-arrest-journalists/ (accessed 1 July 2021).

40 Regulation 2.

In terms of legality of the Regulations under international human rights law, using the revised Declaration, the offences and activities for which surveillance may be carried out are spelt out under Regulations 7(3)(a) to (e) and 16. In addition to this, the categories of people who may be subject to surveillance and time-limit on surveillance operations are provided for under Regulations 4(a)(b) and 14 respectively. In terms of due process, Regulations 17, 18 and 6 deal with examination, use and storage of surveillance data respectively. Regulation 6 also provides for the destruction or erasure of surveillance data while Regulation 19 provides for an oversight function in the Attorney General of the Federation (AGF) but not an independent supervisory authority appointed by and responsible to the legislature. Under the Regulation, the AGF who is a member of the Executive is reported to in terms of surveillance updates in Nigeria. There were also no provisions with respect to precautions that must be taken in cases where surveillance data are found with third parties.

A closer look at the principle of legality and the provisions of the Regulations show that requirements such as definition of offences and activities where surveillance may be carried out, the categories of people that may be surveilled, the time-limit for surveillance operations, due process, and destruction or erasure of surveillance data are provided for. However, the precautions that must be adhered to when surveillance data is with third parties, such as the securitisation of information, is not provided for under the Regulations. In addition to this, there is no independent supervisory authority which is appointed by and responsible to the legislature. Rather, the report to be prepared by law enforcement on surveillance will be submitted for supervision to the AGF and not a legislative committee.

In general, the provisions of Regulation 7(3) provide for various legitimate aims which the judge may rely on in granting of a surveillance request. Some of this includes the grounds of ensuring public safety, prevention of crime, protecting the rights of others, ensuring national security and protecting the economic well-being of Nigerians.[41] Regulation 12 empowers a judge to determine the necessity, adequacy and proportionality of surveillance requests before granting them. While the Regulation provides for both prior and retroactive judicial authorisation with respect to a surveillance request under 12(1), (2), (3) and (4), it does not provide for internal judicial checks. However, Regulation 20 provides for the right to remedy.

There are no clear provisions with respect to transparency and public oversight under the Regulations as only the AGF is to be reported to and not any other independent supervisory authority. Regulations 9 and 11 also require licensees to provide for interception and decryption capabilities. In addition to these, while the Regulations provide for surveillance on the basis of international cooperation under Regulation (7)(3)(e), there are no specific guidelines with respect to such cooperation and how it protects the privacy right of Nigerians. Even though Regulation 5 criminalises unlawful interception of

41 Regulations 7(3)(d), 7(3)(b), 7(3)(a) & 7(3)(d).

communications, Regulation 13(1)(d) could be used to encourage unlawful interception where the judge later grants a retroactive surveillance request.

5.1.2 Assessment of the provisions of the Lawful Interception of Communications Regulations, 2019 (Regulations)

The Regulations may be considered to comply with aspects of international human rights principles with respect to communication surveillance. For example, on the principle of legality, there are provisions for offences and activities when communication surveillance can be carried out; the categories of people that may be surveilled; the time-limit for a surveillance operation; due process safeguards like examination, use and storage of surveillance information and destruction or erasure of surveillance data. However, the Regulation does not provide for safeguards for precautions when surveillance data is handled by third parties as required under Principle 41(3) of the revised Declaration. It also does not provide for independent supervisory authority which is appointed by and responsible to the legislature as required under Principle 41(6)(f) of the Declaration. While some aspects of the principles may have been complied with, non-compliance with the outstanding aspects means that the principle of legality is not complied with.

The Regulations also cover the legitimate grounds for carrying out lawful interception and necessity, adequacy and proportionality requirements in line with the Principle 41(5) of the revised Declaration. They provide for international cooperation and integrity of communications and systems. With respect to the latter, however, the Regulations mandates the use of interceptable systems by service providers and decryption of messages where necessary. These run contrary to the provisions of Principles 41(1) and (2) of the revised Declaration. However, while they provide for prior and retroactive judicial authorisation, there are no provisions as to internal judicial checks with respect to surveillance requests. There are also no clear provisions as to the requirements of 'user notification', transparency, public oversight, and safeguards against illegitimate access. A cumulative assessment of the Regulations alongside international human rights standard on a rights-respecting framework on communication surveillance shows that the Regulation falls short of the necessary requirements of adequately protecting the right to privacy.

In a related judgment on communication surveillance in 2018, the Nigerian Court of Appeal in *Paradigm Initiative & Others v Attorney General of the Federation and others*,[42] considered the constitutionality of section 38 of the Cybercrime Act. The provision gives law enforcement agencies powers to request communication data from service providers without any meaningful checks for such powers.

42 *Paradigm Initiative & others v Attorney General of the Federation and others* CA/L/556/2017 (*Paradigm Initiative* case).

However, while the Court did not find merit in the case of the appellant that the provisions of the section were unconstitutional, Georgewill JCA noted that the provisions of subsections 2(b) and 3 of the Act were problematic. The learned Justice stated:[43]

> There is an overriding need to observe at all times the rights of the citizens to privacy of their communication and any derogation therefrom should be one under due process and adequate legal checks to safeguard the rights of citizens.

While these thoughts by the learned Justice are useful in setting the tone for a rights-respecting law in Nigeria, they partly address the challenges of non-compliance of laws on communication surveillance with international human rights standards in Nigeria. For example, the provisions expressly referred to by the learned Justice focused on just the requirements of prior and retrospective judicial authorisation for surveillance requests. There are several other international human rights law requirements that are yet to be complied with by the provision which also points to the reason why a communication surveillance law that seeks to be rights-respecting ought to be primary, debated before the National Assembly and comprehensive, elaborated on in one single, accessible and sufficiently clear law. The appellate court's decision has however been appealed to the Supreme Court.[44]

5.2 An overview of communication surveillance landscape in South Africa

In addition to section 14 of the Constitution of South Africa that provides for the right to privacy, a number of laws from various sectors also touch on communication surveillance.[45] However, this article focuses more on the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (RICA).

In terms of surveillance practices, there were reports that in 2005, political opposition of the government were indiscriminately surveilled.[46] In other instances, journalists have been at the receiving end of government's arbitrary use of surveillance. In 2010, two journalists Hofstätter and wa Afrika, both of the newspaper *Sunday Times,* were indiscriminately surveilled by the government on the pretext of gun

43 *Paradigm Initiative* case (n 42) 36.

44 D Adeniran 'CSOs head to Supreme Court over Cybercrimes Act' *Order Paper* 2 August 2018 https://www.orderpaper.ng/csos-head-to-supreme-court-over-cyber-crimes-act/ (accessed 16 June 2021).

45 Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (RICA); Protection of Personal Information Act (Act 4 of 2013) (POPI); the Financial Intelligence Central Act of (Act 38 of 2001) (FICA); the Intelligence Services Oversight Act (Act 40 of 1994) (ISOA); the CyberCrimes and CyberSecurity Act (2015) (CAC); The Electronic Communications and Transactions Act (Act 25 of 2002) (ECTA); the General Intelligence Laws Amendment Act (act 11 of 2013) (GILAB); the Criminal Procedure Act (Act 51 of 1977) (CPA) the Films and Publications Act (Act 65 of 1996) (FPA).

46 H Swart 'Secret state: how the government spies on you' *Mail & Guardian* 14 October 2011 https://mg.co.za/article/2011-10-14-secret-state/ (accessed 1 July 2021).

running but facts showed that the surveillance was as a result of how both journalists exposed government corruption.[47] In addition to this, it was reported that two journalists, Marianne Thamm[48] and Jeff Wicks,[49] both working for *Daily Maverick*, a South African investigative newspaper, were being indiscriminately surveilled by the government. This was allegedly due to their work in exposing the corruption within Crime Intelligence, a division of the South African Police Service that tracks criminal offenders.

Thamm and Wicks's surveillance came after the historic decision on communication surveillance delivered by the Constitutional Court of South Africa in the *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*.[50] The case was brought by amaBhungane Centre for Investigative Journalism NPC. Its manager, Sam Sole, was a subject of government surveillance under the provisions of the RICA. The Court found that the RICA did not provide for 'user notification'; ensure judicial independence of the designated judge; provide internal judicial checks on *ex-parte* orders; provide for use, examination, storage and destruction of surveillance data and make special requirements for certain categories of people like practising lawyers or journalists. The provisions of the law were declared unconstitutional.

5.2.1 The Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (RICA)

In South Africa, RICA is the most comprehensive and primary law on communication surveillance. The law is divided into ten chapters: the introductory provisions; prohibition of interception of communications and provision of real-time or archived communication-related information and exceptions; applications for, and issuing of, directions and entry warrants; execution of directions and entry warrants; interception capability and compensation; interception centres, office for interception centres and Internet Service Providers Assistance Fund; duties of telecommunication service provider and customers; general prohibitions and exceptions; criminal proceedings, offences and penalties; and general provisions. Its objectives include regulation of 'interception of certain communications; to regulate the making of

47 J Duncan 'Communications surveillance in South Africa: The case of the Sunday Times newspaper' (2014) *Global Information Society Watch* https://giswatch.org/en/country-report/communications-surveillance/south-africa#_ftn6 (accessed 21 June 2021).

48 A Mitchley 'Sanef condemns alleged illegal surveillance of News24 journalist by Crime Intelligence' *News 24* 8 March 2021 https://www.news24.com/news24/southafrica/news/sanef-condemns-alleged-illegal-surveillance-of-news24-journalist-by-crime-intelligence-20210308 (accessed 21 June 2021).

49 J Etheridge 'Sanef demands that Crime Intelligence stop 'bugging' journalists' *News 24* 19 March 2021 https://www.news24.com/news24/southafrica/news/sanef-demands-that-crime-intelligence-stop-bugging-journalists-20210319 (accessed 21 June 2021).

50 2021 (3) SA 246 (CC).

applications for and the issuing of directions authorising the interception of communications.'

Assessing the various principles under international human rights law on communication surveillance and this law, there are a number of gaps with respect to the compliance of the latter with the former. Considering the seven sub-principles under the requirement for legality, the RICA complies with them only in part. For example, section 16(5)(i) to (v) provides for the specific offences and activities where surveillance may be carried out and information intercepted while section 2 provides for the category of people whose communication may be intercepted. Section 16(2)(f) also provides for the need to indicate a time-limit in a surveillance request while section 30 provides guidance on the examination, use and storage of surveillance data. However, there are no provisions for the necessary precautions for having surveillance data with third parties, destruction or erasure of surveillance data and an independent supervisory authority appointed by and responsible to the legislature.

In terms of a legitimate aim upon which communication surveillance may be carried out, the RICA provides for public safety; the need for prevention of crime; protection of the rights of others; national security and economic well-being.[51] There are also the provisions of section 16 which empowers a designated judge to determine the necessity, adequacy and proportionality of surveillance requests before granting them. Sections 16(1) and 7(4) provide for prior and retroactive judicial authorisation of surveillance requests, respectively. However, the RICA has no provisions with respect to internal judicial checks for *ex-parte* orders.

In addition to this, the RICA does not provide for the right to remedy for a person who has been illegally surveilled under the Act. There are also no provisions in terms of the requirement for transparency which ensures that the law is clear and could be easily monitored by the public for its compliance with the rule of law. For public oversight for surveillance in South Africa, section 37(3) of RICA makes provision for the director of the interception centres established under chapter 6 to coordinate the reports from heads of interception centres which is then submitted to the executive through the Minister and to the legislature through the Chairperson of the standing committee on intelligence.

Section 30(2)(ii) also provides for the integrity of communications and systems which must be provided for by the service provider. Section 16(5)(iv)(a) also provides for international cooperation among states to ensure mutual assistance. Under section 47(1), there is no safeguard against illegitimate access to surveillance data because illegally intercepted communication can still be admissible before the court if it finds it relevant.

51 Sections 16(5)(a)(ii); 16(5)(a)(i)(iv)) of RICA; 16(5)(a)(i-v); 16(5)(ii)) of RICA.

5.2.2 An assessment of the RICA

The judgment of the Constitutional Court in the *Amabhungane* case has been instructive especially with how it sets a jurisprudential tone with respect to rights-respecting laws and communication surveillance. The judgment has provided a springboard for the application of international human rights law in the framing of communication surveillance laws in local contexts. However, in examining the *Amabhungane* case more closely, it appears that while the Court's judgment arrived at impactful judicial orders with respect to the RICA's compliance with international human rights standards, it still missed a number of RICA's other shortcomings.

In terms of its reference to copious aspects of international human rights law, the judgment mirrored the applicable international human rights law that may also be found in the revised Declaration on 'user notification';[52] judicial independence;[53] internal judicial checks on *ex-parte* orders;[54] use, examination, storage and destruction of surveillance data;[55] and special requirements for certain categories of people like practising lawyers or journalists.[56] However, it failed to consider in detail the impacts of other inadequacies such as the necessary precautions for the handling of surveillance data with third parties;[57] provision for an independent supervisory authority appointed by and responsible to the legislature;[58] right to effective remedy;[59] transparency and public oversight;[60] and safeguards for illegitimate access to surveillance data.[61] All of these points to the gaps in the RICA in terms of compliance with international human rights standards on laws on communication surveillance.

5.3 AN OVERVIEW OF COMMUNICATION SURVEILLANCE LANDSCAPE IN UGANDA

In the past, Ugandan laws that seek to regulate digital technologies have been criticised as being non-compliant with international human rights standards.[62] They include the Regulation of Interception of Communications Act, 2010 and the Anti-Terrorism Act, 2002. In terms of surveillance practices in Uganda, in June 2020, Uganda's Defence Ministry stated that it would use 53 per cent of its budget on 'classified expenditure.' It defined such expenditure as 'spending under the

52 Principle 41(6)(d)(e) the revised Declaration.
53 Principle 41(6)(a) of the revised Declaration.
54 Principle 41(6)(a) of the revised Declaration.
55 Principle 41(4) of the revised Declaration.
56 Principle 41(6) of the revised Declaration.
57 Principle 41(3) the revised Declaration.
58 Principle 41(6)(f) the revised Declaration.
59 Principle 41(6)(d) the revised Declaration.
60 Principle 41(6)(f) the revised Declaration.
61 Principle 41(3)) the revised Declaration.

military's covert undertakings.' It is not immediately clear what this means under any law in Uganda. The Ministry is also alleged to have spent close to Shs4 trillion (approximately US$1 125 468 000,00) on classified expenditure and may spend up to Shs1.55 trillion (approximately US$281 367 000,00) on 'defence equipment' in the coming year.[63] In 2019, there were reports that the government of Uganda was actively tracking political opposition in the country.[64]

These reports have been preceded by allegations of surveillance against the Ugandan government. In 2011, state institutions conducted intrusive surveillance on major key opposition leaders and private individuals through a secret operation codenamed *Fungua Macho* which means 'open your eyes' in Swahili.[65] Documents obtained by Privacy International, an international organisation working on privacy rights, have shown the heavy involvement of the Ugandan government in the use of spyware and mass surveillance equipment. In a report published by the organisation in 2015, there were verifiable information on how Ugandan government officials visited Gamma International GmbH headquarters in Munich in 2012. Gamma International is a company that manufactures *FinFisher* – a spyware that has far-reaching privacy intrusive capabilities.[66]

5.3.1 The Regulation of Interception of Communications and Provision of Communication-related Information Act, 2010 (RICA)

In Uganda, the Regulation of Interception of Communications Act, 2010 is the most elaborate law with respect to communication surveillance. One of the major objectives of the Act is to 'provide for the lawful interception and monitoring of certain communications in the course of their transmission through telecommunication.' The law is divided into five major parts and a schedule: the preliminary provisions; control of interception and establishment of a monitoring

62 Unwanted Witness 'Repressive: Uganda's worst cyber laws threatening free expression and privacy', https://www.unwantedwitness.org/download/uploads/REPRESSIVE-UGANDA-WORST-CYBER-LAWS_2.pdf (accessed 21 June 2021); Privacy International 'State of privacy in Uganda' 26 January 2019 https://privacyinternational.org/state-privacy/1013/state-privacy-uganda (accessed 21 June 2021).

63 BH Oluka 'Govt Spends Shs 200bn on Spying Gadgets' *Observer Uganda* 19 October 2019 https://www.observer.ug/news-headlines/40521-govt-spends-shs-200bn-on-spying-gadgets (accessed 21 June 2021).

64 S Solomon 'In Uganda, dissidents adapt to evade Huawei assisted government spying' *Voice of America* 14 November 2019 https://www.voanews.com/africa/uganda-dissidents-adapt-evade-huawei-assisted-government-spying, (accessed 16 June 2021); J Parkinson, N Bariyo, J Chin 'Huawei technicians helped African governments spy on political opponents' *The Wall Street Journal* 15 August 2019 https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017 (accessed 1 July 2021).

65 Privacy International 'For God and my President: state of surveillance in Uganda' October 2015 https://privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf (accessed 21 July 2021).

66 As above.

centre; application for lawful interception of communications; postal articles; and general provisions.

In terms of its compliance with international human rights law, there are a number of aspects of the Act that complies with the principle of legality. For example, the Act provides for the offences and activities where lawful surveillance may be carried out and time-limit for a surveillance operation under sections 5 and 4(3)(e). Other requirements for legality such as provision for the category of people who may be subjected to surveillance; examination, use and storage of surveillance data; the necessary precautions that should be taken when surveillance data is handled by third parties; destruction or erasure of surveillance data and an independent supervisory authority appointed by and responsible to the legislature are not provided for under the Act.

For the principle of legitimate aim, the Act provides for justifications that could lead to surveillance which include public safety (section 5(1)(d)), prevention of crime (section 5(1)(b)), protection of the rights of others (section 5(1)(a)), national security (section 5(1)(c)) and economic well-being (section 5(1)(d)). Sections 5 and 6 of the Act make provisions for a designated judge to apply the principles of necessity, adequacy and proportionality.

While the law provides for the requirement of prior judicial authorisation for surveillance requests, it does not provide for a retroactive judicial authorisation. In addition, it does not provide for 'user notification' and internal judicial checks. The Act also does not make provision for the right to effective remedy, transparency, and public oversight. However, it provides for integrity of communications and systems which must be at the expense of the service provider. It provides for international mutual assistance as a basis for interception under section 5(e) but does not adequately protect against illegitimate access safeguard especially when the provisions of section 8 of the Act is considered.

5.3.2 An assessment of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2010 (RICA)

In terms of compliance with international human rights law standards, Uganda's RICA only provides for two out of the seven sub-principles of legality. It also does not provide for retroactive judicial authorisation (Principle 41(6)(a)), 'user notification' (Principle 41(6)(d)(e)), internal judicial checks with respect to *ex parte* orders (Principle 41(6)(a)), right to effective remedy (Principle 41(6)(d)), transparency and public oversight (Principle 41(6)(f)), examination, use and storage of surveillance data (Principle 41(4)), necessary safeguards when surveillance data is handled by third party (Principle 41(3)), destruction or erasure of surveillance data (Principle 41(4)); and an independent supervisory authority appointed by and responsible to the legislature (Principle 41(6)(f)). These gaps show that the Ugandan RICA is not in compliance with international human rights law on communications surveillance.

6 FRAMING RIGHTS-RESPECTING LAWS ON COMMUNICATION SURVEILLANCE IN NIGERIA, SOUTH AFRICA AND UGANDA

In terms of compliance with international human rights law, using the revised Declaration, Nigeria, South Africa and Uganda do not comply with the requirement of legality. The Ugandan RICA for example does not make provision for the category of people who may be subjected to surveillance; examination, use and storage of surveillance data; the necessary precautions that should be taken when surveillance data is handled by third parties; destruction or erasure of surveillance data and an independent supervisory authority appointed by and responsible to the legislature. In the case of the laws on lawful surveillance for South Africa, they do not provide for the principles of necessary precautions that should be taken when surveillance data is handled by third parties; destruction or erasure of surveillance data and an independent supervisory authority appointed by and responsible to the legislature. In the case of Nigeria, the law does not provide for the principles of necessary precautions that should be taken when surveillance data is handled by third parties and an independent supervisory authority appointed by and responsible to the legislature.

All three countries seem to provide for legitimate aims under the various laws. Most of these aims are those that justify communication surveillance due to the need for ensuring public safety, prevention of crime, protecting the rights of others, ensuring national security and protecting the economic well-being of their people. In addition to these, there seems to be an opportunity for a judge to consider the principles of necessity, adequacy and proportionality of a surveillance request before granting it in each of the laws. With respect to judicial overview and due process, none of the laws provide for 'user notification' after surveillance and internal judicial checks for *ex-parte* orders. While the laws in Nigeria and South Africa provide for the requirement of both prior and retroactive authorisation of a judge in the approval of a surveillance request, Uganda only provides for prior authorisation.

Out of the three countries under assessment, only Nigeria provides for the right to remedy where a surveilled subject feels aggrieved. With respect to the transparency requirement and public oversight, neither Nigeria nor Uganda provides for the former while only South Africa has a considerable provision with respect to the latter. In terms of integrity of communications and systems, Nigeria mandates its licensees to provide for interception and decryption capabilities while Uganda mandates just the former. South Africa does not have such provision contained in the RICA. All of the three countries provide for international cooperation, that is, mutual legal assistance in fighting crime but without adequate guidelines on what such assistance would entail with respect to surveillance. In the same vein, each country provides for the admissibility of illegally intercepted information that could be relevant to a court proceeding. This leaves room for potential abuse by law enforcement agencies who could as a result of these provisions engage in mass and unlawful surveillance.

Given that these requirements are jointly applicable and that part-compliance with them does not suffice, the laws in Nigeria, South Africa and Uganda do not comply with applicable provisions of international human rights law. Drawing from these assessments, there are three major needs that should be met for laws on communication surveillance to be rights-respecting and be framed from a human rights approach.

First, there is a need for an elaborate set of standards with respect to communication surveillance, human rights protection and the responsibilities of states. There have been a number of examples in the past where the African Commission has developed model guidelines and laws with respect to human rights issues.[67] This will improve the prospects of rights-respecting communication laws in the African region in two major ways. One, it will provide an opportunity for the African human rights system to set the tone on an important aspect of human rights in the digital age while also setting clearer directions for states to adapt broad principles of international human rights law to their national legislative frameworks on communication surveillance. Two, it will provide non-state actors with standards to hold states responsible with respect to communication surveillance.

Second, the identified laws with respect to communication surveillance in Nigeria, South Africa and Uganda require urgent reforms in order to comply with international human rights law. This reform will also be necessary for all other legal provisions that bear on state surveillance. Such reform will involve a more inclusive and wide consultations by the legislature that would lead to amendments of old laws or enactment of new ones. For example, Nigeria needs a primary legislation enacted specifically for communication surveillance by the legislature and so do South Africa and Uganda need amendments in various parts of their communication surveillance laws highlighted above.

Third, there is a need to equip major government stakeholders with critical and strategic training on the need for human rights protection in communication surveillance. For example, designated judges will require capacity building with respect to emerging challenges posed by communication surveillance to privacy rights especially in the digital age. This will also be necessary for legislators who make the laws to understand the importance of each provision of such laws. There is also a need to carry out more capacity building with respect to wide powers of the executive to carry out surveillance with more accountability and transparency. This training will ensure that each government stakeholder understands its powers and limits under the law.

67 The Model Law on Access to Information for Africa (2013) https://www.achpr.org/legalinstruments/detail?id=32 24 (24 June 202; Guidelines on Freedom of Association and Assembly (2017) https://www.achpr.org/public/Document/file/English/guidelines_on_freedom_of_association_and_assembly_in_africa_eng.pdf (accessed 24 June 2021); Guidelines on Access to information and Elections in Africa (2017) https://www.achpr.org/public/Document/file/English/guidelines_on_access_to_information_and_elections_in_africa_eng.pdf (accessed 24 June 2021) and the revised Declaration.

7 CONCLUSION

The main goal of this article is to assess the adequacy of laws on communication surveillance and examine the possibilities of framing a rights-respecting reform of these laws through the African human rights system in three African countries: Nigeria, South Africa and Uganda. This is done by focusing on the major international human rights instruments that offer more guidance on the impacts of communication surveillance and how effective the major laws are in each of these countries with respect to compliance with human rights. In the analyses of the provisions of each of these laws in each country, the article concludes that the major international human rights principles on communication surveillance, especially the recently revised Declaration, are not complied with. In a number of instances, the laws comply with aspects of these major principles but still falls short of the requirement of international human rights law on making a law with respect to communication surveillance.

Therefore, there is an urgent need to frame communication surveillance laws on human rights principles and less on paranoia, unchecked state control and arbitrariness. Nigeria, South Africa and Uganda should join other African countries in pushing for a regional set of rights-respecting guidelines or model law on communication surveillance. This process can be championed by the African Commission. In addition to this, each country must embark on thorough reform of its laws not only through amendments and enactments, but also through planned implementation of such reforms. Lastly, each country must commit to training proximate government stakeholders involved in the implementation of communication surveillance laws.